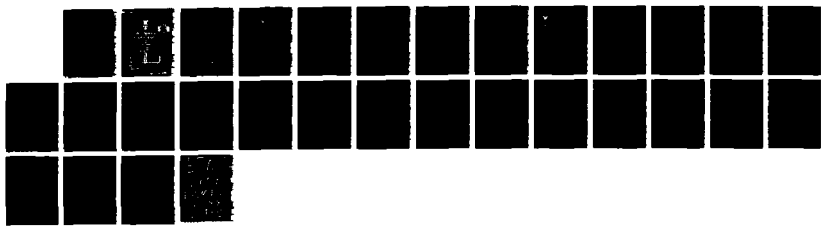
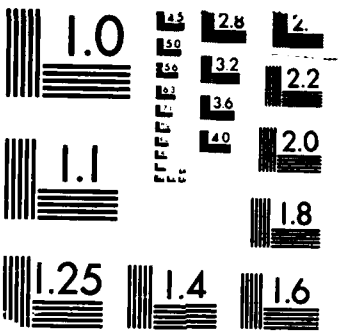
AD-A193 536 EVALUATION OF WATCHDOG SOFTWARE(U) AIR COMMAND AND STAFF COLL MAXWELL AFB AL T C FREEMAN APR 88 ACSC-88-0990 1/1

UNCLASSIFIED F/G 12/5 NL





(2)

AIR COMMAND AND STAFF COLLEGE

STUDENT REPORT

EVALUATION OF WATCHDOG SOFTWARE

MAJOR TIMOTHY C. FREEMAN 88-0990

"insights into tomorrow"

DISCLAIMER

The views and conclusions expressed in this document are those of the author. They are not intended and should not be thought to represent official ideas, attitudes, or policies of any agency of the United States Government. The author has not had special access to official information or ideas and has employed only open-source material available to any writer on this subject.

This document is the property of the United States Government. It is available for distribution to the general public. A loan copy of the document may be obtained from the Air University Interlibrary Loan Service (AUL/LDEX, Maxwell AFB, Alabama, 36112-5564) or the Defense Technical Information Center. Request must include the author's name and complete title of the study.

This document may be reproduced for use in other research reports or educational pursuits contingent upon the following stipulations:

- Reproduction rights do not extend to any copyrighted material that may be contained in the research report..

- All reproduced copies must contain the following credit line: "Reprinted by permission of the Air Command and Staff College."

- All reproduced copies must contain the name(s) of the report's author(s).

- If format modification is necessary to better serve the user's needs, adjustments may be made to this report--this authorization does not extend to copyrighted information or material. The following statement must accompany the modified document: "Adapted from Air Command and Staff College Research Report (number) entitled (title) by (author)."

- This notice must be included with any reproduced or adapted portions of this document.

REPORT NUMBER 88-0990

TITLE EVALUATION OF WATCHDOG SOFTWARE

AUTHOR(S) MAJOR TIMOTHY C. FREEMAN, USA

FACULTY ADVISOR CAPT RON FORD, ACSC/EDP

SPONSOR LTC GREGORY G. CHOBAN, OJCS/J6I

Submitted to the faculty in partial fulfillment of requirements for graduation.

AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY
MAXWELL AFB, AL 36112-5542

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT STATEMENT "A" Approved for public release; Distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) 83-0990	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION AOSC/EDC — 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code)	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION — 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. — PROJECT NO. — TASK NO. — WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
Evaluation of WATCHDOG Software (U)

12. PERSONAL AUTHOR(S)
Timothy C. [illegible]man, Major, USA

13a. TYPE OF REPORT	13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
		1983 February	27

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

A comparative review of Fischer International Corporation's security software, WATCHDOG. Evaluating the access control features of a commercial off the shelf software product to assist JCS in control access to Personal Computers that double as smart terminals in the WWMCCS network.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL AOSC/EDC Maxwell AFB AL	22b. TELEPHONE (Include Area Code) (205) 293-2867 — 22c. OFFICE SYMBOL

DD Form 1473, JUN 86 — Previous editions are obsolete.

TABLE OF CONTENTS

PREFACE

The proliferation of the personal computer (PC) in the workplace being used as smart terminals in network systems is a growing problem for computer security managers. This proliferation of PCs has caused much concern among computer security specialist and has provided an excellent opportunity to evaluate a software product that could assist these managers in controlling access to PCs used as part-time network terminals. Many PC's integrated into the World Wide Military Command and Control System (WWMCCS) fall into this category. The WWMCCS Information Network (WIN) has many locations in the network that use IBM and IBM Compatible PCs as smart terminals and as stand alone computers.

Ms. Debra S. Peterson, Regional Sales Consultant for the Fischer International Systems Corporation and Mr. Joseph Debarthe of Fort Hood's TRADOC Combined Arms Testing Agency (TCATA) have provided a great deal of information and support in my evaluation of the **Watchdog** security system.

ABOUT THE AUTHOR

MAJOR TIMOTHY C. FREEMAN, USA was commissioned in 1971 as an Infantry Officer through the Reserve Officer Training Corp (ROTC) at Stephen F. Austin State University. Sixteen years of service include various command, leadership, and staff positions both in the United States and Europe. Major Freeman attended the Automation Management Officer Course during 1978 and has served seven years in the Automatic Data Processing (ADP) field. In 1978, Major Freeman served as the Chief of the 5th Infantry Division's Division Data Center where he was responsible for the day to day operation, training, and maintenance of the 5th Infantry's computer center servicing over 17,000 members of the Division. During this tour of duty, Major Freeman became interested in Computer Security and became very familiar with the U.S. Army's security methods. In 1984 Major Freeman was selected to serve as the Allied Command Europe Computer Security Manager, responsible for the security of equipment and information contained in over 800 classified computer systems in 14 nations of NATO. Major Freeman was also responsible for preparing and updating ACE security regulations and functioned as the primary staff officer to the SHAPE Chief of Staff for computer and data security.

EXECUTIVE SUMMARY

Part of our College mission is distribution of the students' problem solving products to DOD sponsors and other interested agencies to enhance insight into contemporary, defense related issues. While the College has accepted this product as meeting academic requirements for graduation, the views and opinions expressed or implied are solely those of the author and should not be construed as carrying official sanction.

"insights into tomorrow"

REPORT NUMBER 88-0990

AUTHOR(S) MAJOR TIMOTHY C. FREEMAN, USA

TITLE EVALUATION OF WATCHDOG SOFTWARE

I. Purpose: To evaluate WATCHDOG, a software product designed to assist security managers in monitoring the use of smart terminals and personal computers (PC) that are used in networks.

II. Problem: Personal Computers or smart terminals involved in network operations such as WWMCCS pose a threat to security of the entire system if not monitored very closely by the security manager. Authorized users as well as unauthorized individuals may access these smart terminals and PC's and inadvertently or maliciously cause damage to classified or sensitive data or files.

III. Data: WATCHDOG software provides the security manager with a very good tool with which to manage the devices that can be connected to a network. Evaluation of the Fischer Internation's WATCHDOG, version 4.1, revealed some interesting things concerning access control for personal computers and smart terminals. Identification of the product's specifications show a very complete and well designed security system.

CONTINUED

The specifications of WATCHDOG meet those requirements listed in Department of Defense Trusted Computer System Evaluation Criteria CSC-STD-001-83 for systems handling classified and sensitive information.

IV. Conclusions: Three evaluations of the software, my personal evaluation, an independent laboratory, and a U.S. Army security office found WATCHDOG to be a very capable and valuable product for those Department of Defense users with Personal Computers and smart terminals used in network situations.

V. Recommendations: JCS accept WATCHDOG as the standard software product used by all Departrment of Defense agencies for access control of PC's used as smart terminals in the WWMCCS system.

CHAPTER 1

INTRODUCTION

BACKGROUND

The World Wide Military Command and Control System (WWMCCS) network is being unindated by many remote subscribers using IBM and compatible micro computers. These machines are primarily used as terminals in the WWMCCS network but are very often used in their stand alone capacity. This staff review will focus on a commercial software product that audits all accesses to these smart terminals, or PC's, when they are being used as stand alone computers not operating in the network. The WWMCCS network, (WIN), processes classified and sensitive information that is secured by the use of a complete security system. The terminals used in the network are not automatically secured when they are not operating in the WIN system. Physical and procedural security measures are absolutely essential in the protection of information processed on these machines when used in this mode. WATCHDOG, version 4.1, produced by the Fischer International company of Naples, Florida, is the software product that will be evaluated as a software aid to security. This paper will look at the specific risks involved with micro computers used in networking, the capabilities of the product, a laboratory evaluation of the product, and the applicability of the product for risk reduction and access control.

COMMON NETWORK SECURITY PROBLEMS

Securing a computer is like trying to keep air in a balloon. If there is a leak, no matter how small or how large, all of the air will escape sooner or later and the balloon is no longer valuable for holding air. Either there is security or the data stored in that system or connected systems are at risk (6:20).

"Not so many years ago, computer security meant a guard standing in the entry way to a "strong room" housing the computer" (6:19). This physical security was and is still very useful in some situations, but not the complete answer to a vastly more complicated security problem brought on by networking and smart terminals with mass storage devices. Computer security measures were designed for single application/user situations and were very expensive and of limited value outside their narrow application. Access control is no longer limited to the door to the computer center, but is now responsible for monitoring who uses the computer and which files they access.

THE THREAT ENVIRONMENT

Peter S. Browne wrote about the threat environment in the Summer 1984 issue of Computer Security Journal:

> Threats to the information in networks are not much different than for stand alone or batch systems, but the differences in the way they are manifested and the level of the risks should raise serious concerns...Threats to networks are basically remote threats and anonymous threats. In terms of purposeful or malicious threats, the network offers anonymity to the small but growing group of people who would attempt to penetrate the system. Threats of this type are usually characterized as either passive or active. Passive attacks include analysis of activity to determine importance, sensitivity, and usage patterns. Most of these attacks are mounted simply to penetrate and monitor systems, not for malicious theft, destruction, or fraud. Active attacks involve the changing of data traffic or systems for the purpose of fraud or deliberate damage. While computer security managers have long been aware of these malicious threats, most have not been able to totally control or eliminate these threats (4:81).

The environment that Mr. Browne wrote about is not much different than the environment that the WWMCCS network enjoys. There are many opportunities for users to deliberately or inadvertently compromise the security of the network.

VULNERABILITIES

The vulnerabilities of a distributed network environment such as the WWMCCS network, stem from the very nature of the communications protocols necessary to manage data transfer. The key word is complexity. The large number of nodes, data communication links, and user interfaces provide a very complex environment in which to specify security and control requirements (4:3). In addition, implementation of controls is difficult due to the wide variety of users, systems, and vendors. There is a trend toward multiple sharing of system resources by many different organizations, operating in an environment that is beyond the physical control of systems or communications management. Nanci Reel wrote in the April 1985 issue of Computing for Business, "Network security concepts are complex and security measures vaguely defined becase networks themselves are evolving very rapidly and have resisted standardization" (7:34). The WWMCCS network has evolved and expanded very rapidly. Security against the vulnerabilities may be enhanced by standardization of the security measures and controls placed on the users of the network.

SECURITY MEASURES

PHYSICAL

Physical security of computer resources can take on many different looks. Security of the computer or terminal must be the first priority but the security staff must not overlook the other aspects of physical security. Some of these other aspects can take on the "weakest link in the chain" effect if not properly evaluated and protected; areas such as electrical power, access control to the computer or terminal areas, and storage areas for ADP media. Each of these areas are very important to the overall security of the "system" and take a good deal of the security officer or manager's time in preventing a security breach caused by a lack of physical security.

PROCEDURAL

A major step in assessing and implementing network security involves the written and implied instructions for securing the system. These procedural security measures are expected by users to be informative yet not too

cumbersome for functioning within the system. All the automated aids to security cannot offset the need for complete instructions for all users of the system. Automated security aids can certainly assist the security manager in controlling and monitoring the use of the computer system and determining compliance with the security rules.

All of these security measures are only as good as the security managers that implement them. Their jobs are difficult at best and demand a great deal of time and concentration to catch all the possible security violations committed by users of network assets such as smart terminals or PC's. Automated products such as WATCHDOG can provide the security manager the automated help to maintain system security.

CHAPTER 2

WATCHDOG CAPABILITIES

Because of the risks involved in the use of networks and their related devices and the difficulty of risk reduction, security officers and managers are constantly looking for automated assistance in threat identification and risk reduction. The Fischer company has produced an automated product that will assist the security administrator in identifing and managing the threats and risks created by the introduction of personal computers as smart terminals to networks. WATCHDOG is the automated software product that can assist the security manager in monitoring and managing the PC used as a smart terminal or as a stand-alone computer. The following capabilities of the product have been identified by the Fischer Company in the System Administrator manual, the User documentation manual, and the Quick Installation manual that accompanies the software product (2:--; 3:--; 1:--).

SPECIFICATIONS OF THE PRODUCT

WATCHDOG Version 4.1 has the following system specifications:

SYSTEM-WIDE CONTROLS

a. Option to restrict modifications to AUTOEXEC.BAT files.
b. Option to restrict modifications to CONFIG.SYS file.
c. Option to block utility programs that provide direct access to the disk.
d. Logon Exec allows commands to be automatically executed upon login.
e. Logoff Exec allows commands to be automatically executed upon logoff.

f. Optional or mandatory requirement of Project Description at Login for audit trail accounting.
g. Recording of login/logout date and time by audit trail.
h. Recording of individual program access.
i. Blocks attempts to access the hard disk illegally by means of "booting" the operating system from a floppy disk drive. This prevents any illegal access to a hard disk.
j. Timed screen blank program - can be enabled, and a time limit for blanking the screen after a period of inactivity may be set (Limit may be set from 1-99 minutes).
k. Timed logoff - user will be logged off the system when inactivity exceeds defined time limit (Limit may be set from 1-99 minutes).
l. Internal editor available for modifying internal system files.
m. System option for requiring users to change their User Password at specified time intervals. (Time intervals may be set between 1 and 999 days.)
n. System option for determining the minimum length of User Passwords. (Limits may be set from 4-12 characters.)
o. Applications may be seamlessly embedded in WATCHDOG so that users may access applications with a minimum of keystrokes.
p. A deinstall option allows the System Administrator (SA) to move the WATCHDOG security system to another computer. This option includes facilities for deleting Watchdog areas and also, for converting Watchdog areas into directories as they normally exist under DOS.
q. Backup and restore options for the System Administration data files are available from the SA menu.
r. The program zeroes-out all usable memory each time a user logs off the system. This makes all memory that had been used by the previous user unreadable.

DIRECTORY CONTROLS

a. Addition of secure directories.
b. Description of secure directories
c. Encryption of secure directories is available by assigning an encryption key unique to each directory. WATCHDOG'S encryption technique provides for all data in a directory to be encrypted without user intraction. Encryption process is

totally automatic and transparent to end users; they are not required to know any encryption keys and therefore are not able to compromise its security.
d. Encryption technique provides for data in protected directories to be encrypted both on hard disk storage and on off-line backup media to ensure total security on all media.
e. Exit-to-DOS (Operating System) Permission assigned for each secure directory to prohibit users from accessing the operating system, and to require users to work within the secure WATCHDOG environment.
f. Definition of File Access Permissions of each secure directory. Any combination of the Permissions below may be defined for each directory.
   1) Read Permission - gives users the ability to read files.
   2) Write Permission - gives users the ability to write to an existing file.
   3) Create/Delete Permissions - gives users ability to create and delete new files.
   4) Directories outside of WATCHDOG control may be brought under WATCHDOG protection automatically with a system option executed by the System Administrator.
g. Assignment of area passwords to require an additional password to gain access to a secure directory.
h. Directories outside of WATCHDOG control may be brought under WATCHDOG protection automatically with a system option executed by the System Administrator.

USER ID CONTROLS

a. Assignment of user ID's and user passwords: System Administrator may assign a) primary, b) alternate, and c) one-time passwords for each user.
b. No limit to the number of user ID's per PC.

c. Assignment of permitted directories that users may access.
d. Definition of file access permissions for each user within each permitted area.
e. Exit-to-DOS Permission may be defined for each user or for certain permitted areas of that user.

SYSTEM PROFILE REPORTS

a. Available only to the System Administrator.
b. Seven available reports for use by the SA in reviewing system, area and user definitions:
   1) System Permissions
   2) Areas and Permisssions
   3) Areas and Passwords
   4) User ID's and Passwords
   5) Areas by user ID's
   6) User ID's by Areas
   7) Comprehensive
c. System Administrator data collection worksheets available.

UTILITY SELECTION CONTROLS

Utility functions are available to users for system maintenance, as defined by the System Administrator. Each utility may have a password assigned to control its use. Utilities include:

a. CHKDSK
b. TREE
c. Encrypted BACKUP
d. Encrypted RESTORE
e. Edit AUTOEXEC.BAT
f. Edit CONFIG.SYS
g. User Supplied Command

AUDIT TRAIL

a. Audit Trail information is available only to the System Administrator.

b. Monitors PC usage for security and accounting purposes. The following specific data is recorded:

1) User ID
2) Area or (Directory)
3) Project ID
4) Program execution
5) Date in
6) Time in
7) Date out
8) Time out
9) Elapsed time

c. A report generator is included so the System Administrator may format the data in a custom report tailored to their specifications. Options for comprehensive, detail, session and summary reports are available. Approximately 100 report formats are available with WATCHDOG report generator.

d. A Report format may be saved as a Report Set for repeated use of the same format.

e. Exception reporting is available for reporting inappropriate system activity. Exception data recorded are:

1) WATCHDOG security violations
2) Users guessing ID's and passwords
3) Users guessing area passwords
4) Forced logout
5) Evidence fo attempt to alter audit trail file contents
6) Attempted violation of user file access permissions
7) Use of the DOS commands specified on the Utility Selection Menu
8) All activity by the System Administrator is monitored and recorded.

f. The System Administrator may extract the audit trail file in a text format which can then be used with a data base management program to accommodate additional reporting requirements.

g. Audit Trail reports also permit project accounting. In addition to helping users organize and separate PC-related tasks, Project IDs allow the System Administrator to track user activity and PC usage by specific tasks.

SYSTEM LIBRARY

a. Feature provides a program library or libraries for storing programs that will be used by more than one user. Provides the benefit of many users sharing programs without compromising the security of any directory where protected files are stored.
b. Provides better utilization of hard disk space.

MAILBOX

Provides a method of internal electronic mail communication. Confidential messages may be sent between individual users or groups of users. Internal editor is included for easy composition of all messages and notes.

MENU BUILDER

This feature provides a method of creating a menu structure for each secure directory. This provides for convenient selection of programs, batch files, and subordinate subdirectories. Also provided is an inproved method of organizing area options which supports multiple levels of menus within each area.

USER INTERFACE

a. Users are required to enter ID's and passwords immediately upon system start up. Users can not access protected data without initial login.
b. All area selections are menu driven and system functions are selected by function keys.
c. Help screens available for immediate assistance to users.
d. Users cannot accidentally or maliciously format hard disk.
e. WATCHDOG Tools is accessed by Function Key 4 from the Area
Menu and Sub-menu and allows users to access audit trail information related to their own system activity only. WATCHDOG Tools also allows users to change their Project IDs and their User Password.

SYSTEM COMPATIBILITY

a. Personal Computers:

IBM PC AT	IBM AT/370
IBM PC w/external HD	IBM PC 3270
IBM AT & T PC	IBM AT & T PC 6300
COMPAQ	COMPAQ PLUS
COMPAQ DESKPRO	COMPAQ 286
ITT XTRA	Sperry PC
NCR PC6	NCR PC8
WYSE PC	TELEX PC
Zenith 150	Zenith 155
Zenith 248	Zenith 120 w/IBM Emulation

Any other 100% IBM/PC Compatible Computer

b. Operating System:
PC-DOS 2.0,2.1,3.0,3.1,3.2
MS-DOS 2.0,2.1,3.0,3.1

C. Disk Drive:
Diskette drive - 1 required
Hard disk drive - 1 required (may be internal or add on storage units)
Supports multiple hard disks on same CPU

Supports IBM compatible tapes and drives
Supports removable cartridge system

d. Other Hardward:
Supports monochrome and color monitors
Supports a mouse
Supports any IBM compatible printer with 80 columns or more

COSTS

WATCHDOG is available on GSA contract for $182.90 per copy. This compares to the retail price of $295.00 per copy. The GSA contract number is GS00K87AGS6092. Multiple copy licenses are available for volume purchases. Maintenance agreements can be provided by Fisher on an annual fee basis and provide program release upgrades as they become available at no additional charge and a telephone hot-line for maintenance and technical support services.

CHAPTER 3

PRODUCT EVALUATIONS

The following pages include three different evaluations of WATCHDOG. First, a personal evaluation; second, a laboratory evaluation by DATAPRO Corporation, and finally, a review by the security section of TCATA, Ft. Hood, Texas.

PERSONAL EVALUATION

For my evaluation of WATCHDOG, I installed the software on a Zenith 150 personal computer with a 20-Megabyte hard disk and 512K bytes of RAM, running MS-DOS 3.0. Before installing the product, I carefully read and studied the documentation books provided with the software. The documentation was straight forward and easy to understand. The results of my evaluation are reported in a simular format to the format used by DATAPRO Research Corporation in their evaluation of this product.

INSTALLATION

Installation was easily accomplished with only minor problems caused by my not reading the prompts provided on the screen and the information provided in the 1st-Time Quick Installation Manual (1:--). The hard disk was reformatted for this test so there were no existing files to modify and the installation went very quickly (3 minutes). Under the System Administrator function I added two users to the system and defined four areas to each user. Each user had a directory outside of WATCHDOG, a Create/Delete permission directory, and two files in a directory with Read Only permission. Encryption keys were set and passwords were assigned for each file for each user. This was done to make a very small system as complicated as possible for an evaluation of user ease.

PERFORMANCE

After I had set up the WATCHDOG system, I started using the system as a User and entered data into my files. I tried to browse into the other User's files and was not permitted by the WATCHDOG system to enter any file except the Read Only files for which I had access. Ater exiting the system, I rebooted the PC from dirve A using a DOS utility diskette, NORTON UTILITIES. I tried several ways to get into the WATCHDOG files on the "C" drive without any success. I tried to delete the files, reformat the "C" drive, and view the data all without success. With WATCHDOG installed, the system would not recognize "C" drive. I then powered down the PC ,and as a user might do, I started the computer with a word processor program in drive "A". I used that application program and saved a file to a disk in the "B" drive. After successfully completing this task, I then executed a warm reboot of the PC using the hard drive and entered as the System Administrator(SA). I wanted to examine the audit capabilities and the reports available to the security manager. There were a least 100 reports available to the SA. This appears to be a gold mine of information available to a security manager, but the information is much the same on all of the reports. There are just a lot of ways to display the same information. The SA can make special report formats and save them as automatic reports. This will save a lot of time in reading through security reports trying to find meaningful information. When I printed out my first report, I could not find an entry for the application program that I ran when I rebooted the system. This did not seem right, so I went back to the documentation and found that controlled diskette booting is an option that has to be set in the installation. The system is capable of monitoring these accesses to the machine via the "A" or "B" drives, making the system even more useful for controlling every access to the PC.

ANALYSIS

I personally found that the WATCHDOG software was extremely easy to use both as a System Administrator and as a user. The software provides user identification and authentication, discretionary access control, object reuse, and audit requirements specified by the DOD Trusted Computer System Evaluation Criteria to at least the C2 level and possibly higher. The software is very functional and will provide the security manager a valuable tool in combating unauthorized use of PC's or smart terminals. A shortfall of the current system is that WATCHDOG is not available as

firmware for those PC's without a hard drive. This improvement would eliminate all possibility of gaining access to the computer without an audit record.

DATAPRO EVALUATION

The following is a portion of a laboratory evaluation report produced by DATAPRO Research Corporation, Delran, NJ in their evaluation of WATCHDOG, Version 4.1 (5:102-103).

> For this update, we examined Version 4.1 to test the latest system enhancements. We installed and tested the new version on an IBM PC XT system with 512K bytes of RAM, running MS-DOS 2.1. Our experience with the product follows.
>
> Installation
>
> WATCHDOG'S installation was not difficult, although there were more programs to transfer to the hard disk than before. The system itself is more extensive; however, we still only needed to initiate the INSTALL program on a disk in drive A and respond to a few easy prompts... The operational programs were automatically transferred to the hard sdisk, and the necessary files and directories were set up by the INSTALL program. The CONFIG.SYS and the AUTOEXEC.BAT files were then modified by INSTALL to allow for WATCHDOG. In five minutes, we were set up as the System Administrator (SA), and were ready to start defining areas and adding users.
>
> Performance
>
> We added six users to the system and defined several areas. We could number any area from one to 256, the maximum number of areas that can be established. The process required to add or change the configuration of these areas has been simplified and there is much more "hand-holding" throughout. Also, function keys can be used for all choice (or menu) selections...
> Daily functions, such as controlling program and information access through encryption and access

restriction, tested flawlessly as in our previous test. The encryption process is transparent to the user, and there is no slowing of any disk process. We tried to gain access to programs, files, and directories from the DOS level, but were always denied access. We could find no way to gain access illegally. We tried bypassing the WATCHDOG system by booting up a DOS diskette in the A drive, but all programs and files maintained in a protected area were still unusable and remained encrypted.
WATCHDOG improvements include multiarea log on ability; system library expansion; specified program usage audit; and additional audit formats. However, we feel the key improvement is the multiarea log on function. It permits greater flexibility and ease in running programs and accessing files that might not always be in the system library or in the user's directory at that time. It allows data and program access without having to leave one area and go to another, and often tedious and disk space-consuming procedure of copying from one area to another. The expanded system library is the second big improvement. It is a general directory that is automatically made available to all WATCHDOG system users. Selectively restricted system libraries are established which certain users or groups of users may access. Users with similar interests and needs can access the same data and files, while the data is still protected against those who have no need for it...

Product Analysis

Fischer International is [sic] made many improvements in Version 4.1 of WATCHDOG. There is a wider range of tools for restricting and granting access to programs, files, and directories either by password use, read/write/create access restriction, and/or encryption. Naturally, the integrity of all password-based microcomputer security systems depends upon keeping all passwords secret. Considering that, WATCHDOG provides a sophisticated set of tools for constructing as tight a security system as one is likely to expect on the average microcomputer. If care is taken in planning and executing the SA functions, WATCHDOG would be an excellent shield against

improper microcomputer use. WATCHDOG is ideally suited for multiuser microcomputers.

"TCATA" EVALUATION

The following evaluation is extracted from a research paper done by Mr. Joseph Dean Debarthe of the Automation and Information Management Directorate of Headquarters, TCATA, Fort Hood, Texas during November 1987 (10:1-24). The TCATA evaluation identified 15 of the specifications identified in Chapter 3 that were most advantageous and important to their operation.

> In the recent years the Army has tended to gravitate toward using PC's in the work place. This proliferation has become a major security concern because of the total lack of data security on Personnel Computers. This lack of security allows anyone who has physical access to get to and remove any information from any PC. This presents a security problem for the Army...This concern for security has been transformed into requirements for PC security within the Army regulations, most notably in the latest addition of AR 380-380 and the Automation Security for Saml1 Computers document produced by U.S. Army Intelligence Command 902 Military Intelligence Group.
>
> In compliance with these regulations AIMD has been tasked to evaluate security packages available and make a recommendation to purchase a security package for TCATA wide use...
>
> The only system tested that meets the requirements as described in section 4 (ITEMS 1 - 6) is WATCHDOG. This Security Package is the most versatile system found to date...
>
> WATCHDOG'S directions were somewhat confusing, but the customer support was excellent and enabled me to overcome any problem that occurred in the installation process. If this support is an example of what to expect from them after purchasing the product, this one drawback (difficulty in installation) is adequately covered and is of minimal [sic] concerned.
>
> During the course of evaluating these

systems, many rumors about the WATCHDOG Security package have circulated. Each rumor has been checked out by attempting to defeat the system as rumored or by doing the operation rumored not possible. In each case the WATCHDOG system circumvented all attempts to improperly gain access to unauthorized areas or presented no adverse impact to normal operations. These rumors were:

1). Access to "C" drive using PC tools or NORTON when booting up from "A" drive. Not true, access was denied when unauthorized attempts made.

2). Access to unauthorized areas within "C" drive when authorized to use DOS commands. Not true, access denied when unauthorized attempts made.

3). WATCHDOG will not work on a Local Area Network (LAN). Not true, tested on Unit Mannings LAN and worked without problems.

4). WATCHDOG will not allow transfer of documents or data to or from the Mainframe. Not true, transferred documents to and from the mainframe from the PC with WATCHDOG installed.

5). WATCHDOG will not work on a PIPE. Not true, tested on a PIPE with WATCHDOG installed and it worked properly.

WATCHDOG has been placed on 5 different Zenith 248 PC's for testing purposes. None of the people using these systems have had any adverse effects caused by the addition of the WATCHDOG system...

AIMD is in the unique position to influence which PC Security System is used within TCATA. I presently feel that WATCHDOG should be purchased and used exclusively within TCATA because it is versatile enough to meet the varied security requirements within our organization.

CHAPTER 4

CONCLUSIONS ABOUT "WATCHDOG"

FINDINGS

Automated aids to security can greatly assist security managers and users in keeping sensitive and classified information secure. WATCHDOG, software provides the security manager with a very good tool with which to manage the devices that can be connected to a network.

WATCHDOG allows the Security Manager to appoint a system supervisor who can control all aspects of PC usage by providing all the necessary tools for monitoring, controlling, and reporting all accesses to the PC. These tools are easily manageable by the WATCHDOG System Administrator who is the only person allowed by the software to set permissions and provide access credentials.

The software provides the System Administrator more than adequate report information in a large number of formats (100). These reports present the information necessary for security managers to audit PC usage and identify security violations and violators. WATCHDOG software collects and stores large amounts of information and allows the security manager the privilege of selecting what information is considered important. Even with this comprehensive ability, authorized users of the smart terminals and PC's are not hindered nor slowed down by the software.

WATCHDOG, at a cost of $182.00 per copy, is relatively inexpensive to purchase and maintain. The Fischer International company provides adequate software support to owners of the software. Program release upgrades are provided at no additional costs. Fischer International also provides a telephone hot-line for maintenance and technical support services.

CONCLUSIONS

Personal computers or smart terminals involved in network operations such as WWMCCS pose a threat to security of the entire system if not monitored very closely by the security manager. Evaluation of the Fischer International's WATCHDOG, version 4.1 revealed some interesting aspects concerning access control for personal computers and smart terminals.

Identification of the product's specifications show a very complete and well designed security system. The specifications of WATCHDOG meet those requirements listed in Department of Defense Trusted Computer System Evaluation Criteria CSC-STD-001-83 for systems handling classified and sensitive information (8:--).

Three evaluations of the software, my personal evaluation, an independent laboratory, and a U.S. Army security office found WATCHDOG to be a very capable and valuable product for those Department of Defense users with Personal Computers used as smart terminals in network situations.

BIBLIOGRAPHY

Books

1. Fischer International Systems Corporation. Watchdog PC Data Getting Started: 1st-Time Quick Installation. Naples, Florida, 1985.

2. -----. Watchdog PC Data Systems Administrator Guide. Naples, Florida, 1985.

3. -----. Watchdog PC Data User Guide. Naples, Florida, 1985.

Articles and Periodicals

4. Browne, Peter S. "How to Manage the Network Security Problem." Computer Security Journal, Summer 1984, pp. 77-87.

5. Datapro Research Corporation. Datapro Reports on Informatin Security: Fischer International Systems Corporaton Watchdog, Deltran, New Jersey, July 1987.

6. Kaiser, W. Garry. "The Making of a B2 System." Data Processing and Communications Security, Winter 1987, pp. 19-27.

7. Reel, Nancy. "Data Security: Can Your Computer Keep a Secret?" Computing For Business, April 1985, pp. 34-45.

Official Documents

8. U.S. Department of Defense Computer Evaluation Center. Department of Defense Trusted Computer System Evaluation Criteria. CSC-STD-001-83. Fort George G. Meade, MD 20755: The Center, August 1983.

9. U.S. Department of Defense. Security Requirements for Automation Data Processing (ADP) Systems. DOD Directive 5200.28. Washington: Department of Defense, December 1972.

Unpublished Material

10. Debarthe, Joseph Dean. "PC Security for TCATA." Research Paper, HQ TCATA, Automation and Information Management Directorate, 1987.

END

DATE

FILMED

8-88

DTIC